SonicWALL High Availability

For the SonicWALL GX, the SonicWALL PRO, and the SonicWALL PRO-VX

SONICWALL

Contents

High Availability

A reliable Internet connection has become a mission critical requirement for today's modern business. Internet connections today are used for accessing important real-time data for decision-making, reaching E-commerce customers, connecting with business partners, and extending communications across the distributed enterprise.

The loss of this mission critical connection can have serious, and sometimes disastrous, consequences on an organization.The following applications are examples of the mission critical nature of an Internet connection today:

- An Internet connection that provides customer access to an E-commerce site. In this case, connection downtime results in lost revenue.
- An Internet connection used to connect to business partners or an application service provider (ASP). Connection downtime can significantly disrupt business activities.
- Internet connections that provide access to critical resources for remote offices, telecommuters and mobile workers. Connection downtime can result in lower productivity for remote users.

Given the mission critical nature of many Internet connections, each element of the Internet connection needs to be highly reliable. SonicWALL **High Availability** adds to the award-winning SonicWALL Internet security solution by assuring a highly reliable and secure connection to the Internet.

SonicWALL **High Availability** is standard on the SonicWALL PRO-VX and the GX product line. It is available as an upgrade for the SonicWALL PRO. SonicWALL **High Availability** eliminates network downtime by allowing the configuration of two SonicWALLs (one primary and one backup) as a **High Availability** pair. In this configuration, the backup SonicWALL monitors the primary SonicWALL and takes over operation in the event of a failure. This ensures a secure and reliable connection between the protected network and the Internet.

Getting Started with High Availability

Before Configuring High Availability

Before attempting to configure two SonicWALLs as a **High Availability** pair, check the following requirements:

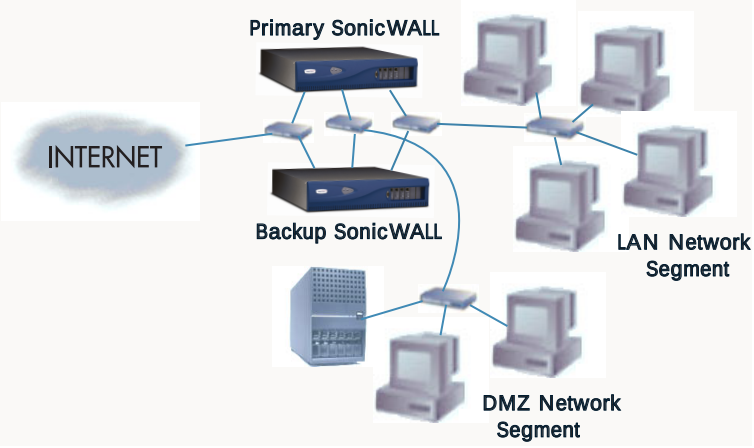
- You have two (2) SonicWALL GX250, two (2) GX650, two (2) PRO, or two (2) PRO-Vx Internet Security Appliances. The **High Availability** pair must consist of two identical SonicWALL models.
- You have at least one (1) valid, static IP address available from your Internet Service Provider (ISP). Two (2) valid, static IP addresses are required to remotely manage both the primary SonicWALL and the backup SonicWALL.

***Note**: SonicWALL **High Availability** does not support dynamic IP address assignment from your ISP.*

- Each SonicWALL in the **High Availability** pair must have the same firmware version installed.
- Each SonicWALL in the **High Availability** pair must have the same upgrades and subscriptions enabled. If the backup unit does not have the same upgrades and subscriptions enabled, these functions are not supported in the event of a failure of the primary SonicWALL.

Network Configuration for High Availability Pair

The following diagram illustrates the network configuration for a **High Availability** pair:

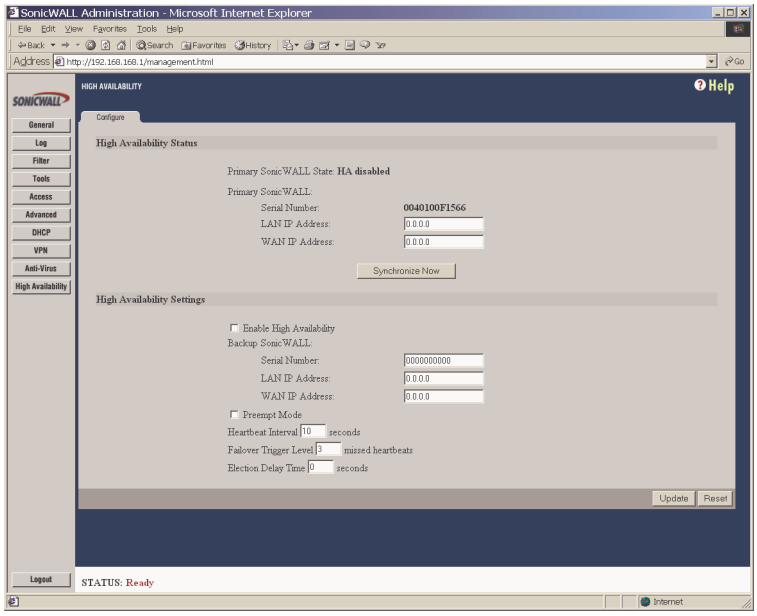


All SonicWALL ports being used must be connected together with a hub or switch. Each SonicWALL must have a unique LAN IP Address on the same LAN subnet. If each SonicWALL has a unique WAN IP Address for remote management, the WAN IP Addresses must be in the same subnet.

Note: The two SonicWALLs in the **High Availability** pair sends "heartbeats" over the LAN network segment. The **High Availability** feature does not function if the LAN ports are not connected together.

Configuring High Availability on the Primary SonicWALL

Click **High Availability** on the left side of the SonicWALL browser window, and then click **Configure** at the top of the window.



The top half of the window displays the primary SonicWALL serial number and network settings. The bottom half of the window displays the backup SonicWALL information boxes. To configure **High Availability**, follow the steps below:

1. Connect the primary SonicWALL and the backup SonicWALL to the network, but leave the power turned off on both units.
2. Turn on the primary SonicWALL unit and wait for the diagnostics cycle to complete. Configure all of the settings in the primary SonicWALL before configuring **High Availability**.
3. Click **High Availability** on the left and begin configuring the following settings for the primary SonicWALL:

- **LAN IP Address** - This is a unique IP address for accessing the primary SonicWALL from the LAN whether it is **Active** or **Idle**.

***Note**: This IP address is different from the IP address used to contact the SonicWALL in the General Network settings.*

- **WAN IP Address (Optional)** - This is a unique WAN IP address used to remotely manage the primary SonicWALL whether it is **Active** or **Idle**.

***Note**: The **Synchronize Now** button is used for diagnostics and troubleshooting purposes and is not required for initial configuration.*

4. In the Web Management interface for the primary SonicWALL, configure the backup SonicWALL settings as follows:

- **Serial Number** - Enter the serial number of the backup SonicWALL.
- **LAN IP Address** - The unique LAN IP address used to access and manage the backup SonicWALL whether it is **Active** or **Idle**.

***Note**: This IP address is different from the IP address used to contact the SonicWALL in the General Network settings.*

- **WAN IP Address (Optional)** - This is a unique WAN IP address used to remotely manage the primary SonicWALL whether it is **Active** or **Idle**.

5. Check the **Preempt mode** checkbox if you want the primary to SonicWALL to takeover from the backup SonicWALL whenever the primary becomes available (for example, after recovering from a failure and restarting). If this option is not used, the backup SonicWALL remains the active SonicWALL.

***Note**: The primary and backup SonicWALLs use a "heartbeat" signal to communicate with one another. This heartbeat is sent between the SonicWALLs over the network segment connected to the LAN ports of the two SonicWALLs. The interruption of this heartbeat signal triggers the backup SonicWALL to take over operation from the active unit of the **High Availability** pair. The time required for the backup SonicWALL to take over from the active unit depends on the **Heartbeat Interval** and the **Failover Trigger** Level.*

6. Enter the **Heartbeat Interval** time in seconds. Use a value between 3 seconds and 255 seconds. This interval is the amount of time in seconds that elapses between heartbeats passed between the two SonicWALLs in the **High Availability** pair.

7. Enter the **Failover Trigger Level** in terms of the number of missed heartbeats. Use a value between 2 and 99 missed heartbeats. When the backup unit detects this number of consecutive missed heartbeats, the backup SonicWALL takes over operation from the active unit.

Example: Assume that the **Heartbeat Interval** and the **Failover Trigger Level** are 5 seconds and 2 missed heartbeats respectively. Based on these values, the backup SonicWALL takes over from the active unit after 10 seconds in the event of a failure in the active unit.

8. Enter the **Active SonicWALL Detection Time** in seconds using a value between 0 and 300. The default value of 0 is correct in most cases.When any SonicWALL (primary or backup) becomes active after bootup, it looks for an active SonicWALL configured for High Availability on the network. If another SonicWALL is active, the SonicWALL that is booting up transitions to the **Idle** mode. In some cases, there may be a delay in locating another SonicWALL due to network delays or problems with hubs or switches.You can configure either the primary or backup SonicWALL to allow an increment of time (in seconds) to look for another SonicWALL configured for **High Availability** on the network. You may enter a value between 0 and 300 seconds, but the default value of 0 seconds is sufficient in most cases.
9. Click **Update**. Once the SonicWALL has been updated, a message confirming the update is displayed at the bottom of the browser window.

***Note**: It is important that during initial configuration, the backup SonicWALL has not been previously configured for use. If the backup SonicWALL has previous network settings, it is recommended to reset the SonicWALL to the factory default settings using **Restore Factory Default Settings** located in the **Tools** section. Additionally, the password must be changed back to the default password of "password" using the **Password** tab in the **General** section.*

10. Power on the backup SonicWALL used for **High Availability**. After completing the diagnostic cycle, the primary SonicWALL auto-detects the presence of the backup SonicWALL and synchronizes the settings.
11. To confirm that the synchronization is successful, check the primary SonicWALL log for a **High Availability** confirmation message. Alternatively, you can log into the backup SonicWALL using its unique LAN IP address and confirm that it is the backup SonicWALL.

If the primary SonicWALL fails to synchronize with the backup, an error message is displayed at the bottom of the screen. An error message also appears on the **Status** tab. To view the error message on the **Status** tab, click **General** on the left side of the browser and then **Status** at the top of the window.

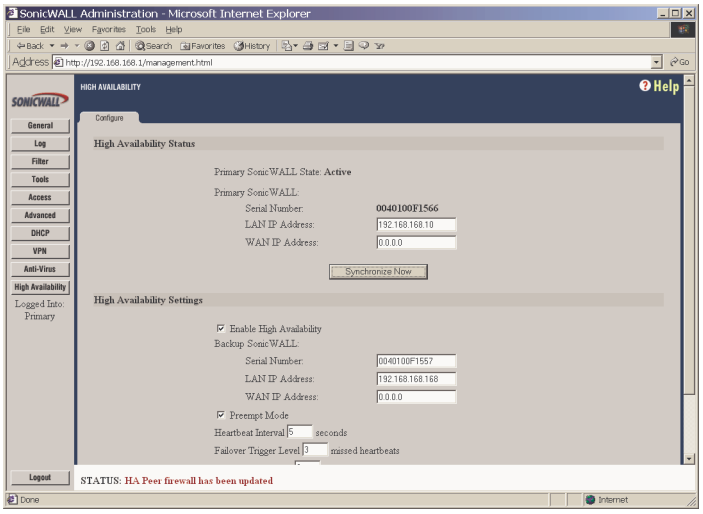
To check the backup SonicWALL firmware version or serial number, log into the backup SonicWALL, click **General** on the left side of the browser window and then click **Status** at the top of the window. Both the firmware version and the SonicWALL serial number are displayed at the top of the window.

If the backup SonicWALL serial number was incorrectly specified in the primary SonicWALL Web Management Interface, log into the primary SonicWALL and correct the backup SonicWALL Serial Number field.

At this point, you have successfully configured your two SonicWALLs as a **High Availability** pair. In the event of a failure in the primary unit, the backup unit takes over operation and maintains the connection between the protected network and the Internet.

Configuration Changes

Configuration changes for the **High Availability** pair can be made on the primary or the backup SonicWALL. The primary and backup SonicWALL appliances are accessible from their unique IP addresses. A label indicates which SonicWALL appliance is accessed.



***Note**: If you change the IP address of either SonicWALL, synchronization cannot occur between the two SonicWALLs without updating the changes manually in the High Availability configuration.*

Synchronizing Changes between the Primary and Backup SonicWALLs

Changes made to the Primary or Backup firewall are synchronized automatically between the two firewalls. If you click **Synchronize Now**,

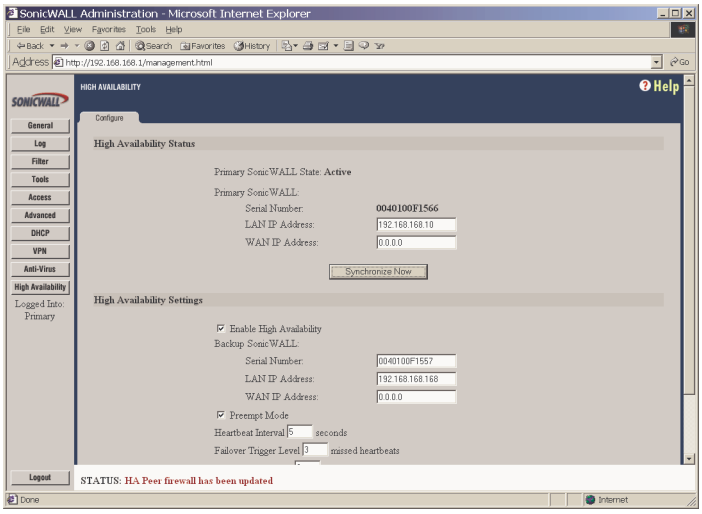
the Backup SonicWall restarts and becomes temporarily unavailable for use as a backup firewall.

High Availability Status

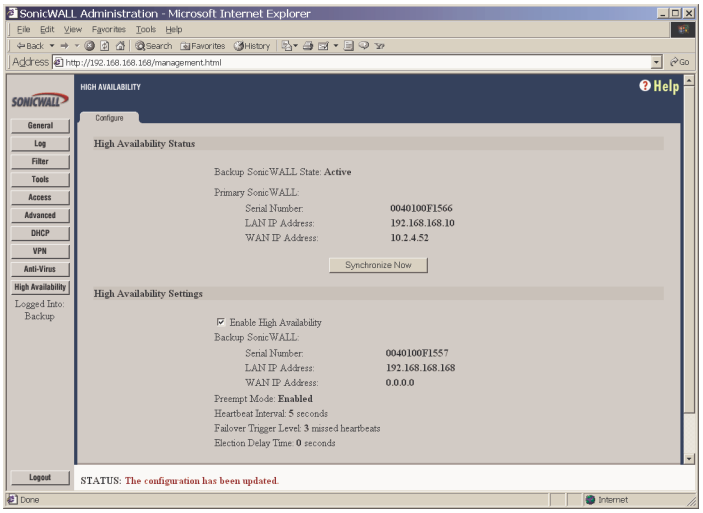
If failure of the primary SonicWALL occurs, the backup SonicWALL assumes the primary SonicWALL LAN and WAN IP Addresses. There are three primary methods to check the status of the High Availability pair: the **High Availability Status** window, **E-mail Alerts** and **View Log**. These methods are described in the following sections.

High Availability Status Window

One method to determine which SonicWALL is active is to check the **High Availability Status** page for the **High Availability** pair. To view the **High Availability Status** window, you can log into the primary or backup SonicWALL LAN IP Address. Click **High Availability** on the left side of the browser window and then click **Configure** at the top of the window. If the primary SonicWALL is active, the first line in the status window above indicates that the primary SonicWALL is currently **Active**.



If the backup SonicWALL is active, the first line changes to reflect the active status of the backup as shown below:



The first line in the status window indicates that the backup SonicWALL is currently **Active**. It is also possible to check the status of the backup SonicWALL by logging into the **LAN IP Address** of the backup SonicWALL. If the primary SonicWALL is operating normally, the status window indicates that the backup SonicWALL is currently **Idle**. If the backup has taken over for the primary, this window indicates that the backup is currently **Active**.

***Note**: In the event of a failure in the primary SonicWALL, you may access the Web Management Interface of the backup SonicWALL at the primary SonicWALL **LAN IP Address** or at the backup **SonicWALL LAN IP Address**. When the primary SonicWALL restarts after a failure, it is accessible using the third IP address created during configuration. If preempt mode is enabled, the primary SonicWALL becomes the active firewall and the backup firewall returns to idle status.*

E-mail Alerts Indicating Status Change

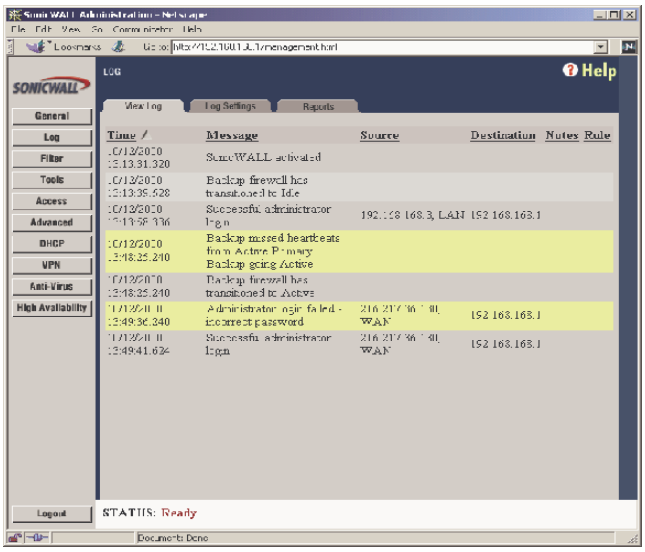
If you have configured the primary SonicWALL to send E-mail alerts, you receive alert E-mails when there is a change in the status of the **High Availability** pair. For example, when the backup SonicWALL takes over for the primary after a failure, an E-mail alert is sent indicating that the backup has transitioned from **Idle** to **Active**. If the primary SonicWALL subsequently resumes operation after that failure, and **Preempt Mode** has been enabled, the primary SonicWALL takes over and another E-mail

alert is sent to the administrator indicating that the primary has pre-empted the backup.

View Log

The SonicWALL also maintains an event log that displays these **High Availability** events in addition to other status messages and possible security threats. This log may be viewed with a browser using the SonicWALL Web Management Interface or it may be automatically sent to the administrator's E-mail address.

To view the SonicWALL log, click **Log** on the left side of the browser window and then click on **View Log** at the top of the window.

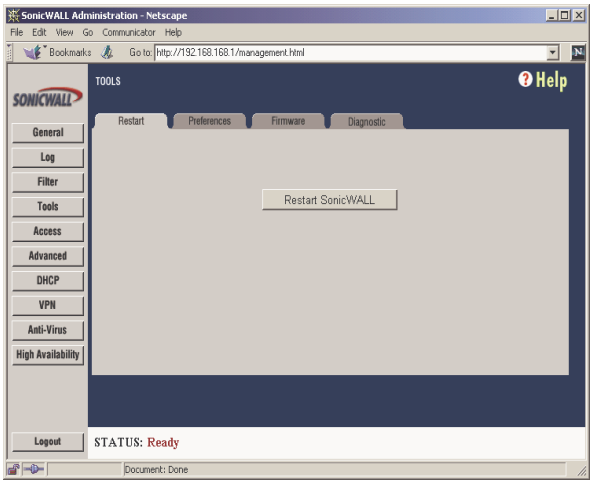


Forcing Transitions

In some cases, it may be necessary to force a transition from one active SonicWALL to another – for example, to force the primary SonicWALL to become active again after a failure when **Preempt Mode** has not been enabled, or to force the backup SonicWALL to become active in order to do preventative maintenance on the primary SonicWALL.

To force such a transition, it is necessary to interrupt the heartbeat from the currently active SonicWALL. This may be accomplished by disconnecting the active SonicWALL's LAN port, by shutting off power on the currently active unit, or by restarting it from the Web Management Interface. In all of these cases, heartbeats from the active SonicWALL are interrupted, which forces the currently **Idle** unit to become **Active**.

To restart the active SonicWALL, log into the primary SonicWALL LAN IP Address and click **Tools** on the left side of the browser window and then click **Restart** at the top of the window.



Click **Restart SonicWALL**, then **Yes** to confirm the restart. Once the active SonicWALL restarts, the other SonicWALL in the **High Availability** pair takes over operation.

***Note**: If the **Preempt Mode** checkbox has been checked for the primary SonicWALL, the primary unit takes over operation from the backup unit after the restart is complete.*

Configuration Notes

- **Changing Password** - Do not change the password on the Backup firewall when it is in Idle condition. Changing the password prevents communication between the firewalls.
- If you are configuring the SonicWALL in **Standard** mode on the network, an additional IP address is necessary for the High Availability configuration.
- Auto Update - If Auto Update is enabled for firmware upgrades, the Primary SonicWALL should be upgraded first. And during the upgrade, the backup SonicWALL should be disconnected from the LAN or turned off. When the firmware upgrade is performed on the backup SonicWALL, the Primary SonicWALL should be disconnected from the network or turned off.

High Availability Activation Key

Register and create a mysonicwall.com user account at <http://www.mysonicwall.com>to receive a High Availability Upgrade Key for the SonicWALL PRO. The SonicWALL GX and PRO-VX do not require activation.

SonicWALL, Inc.
1160 Bordeaux Drive
Sunnyvale, CA 94089-1209
Phone: 408-745-9600
Fax: 408-745-9300
E-mail: sales@sonicwall.com
Web: http://www.sonicwall.com

Part # 232-000094-00
Rev B. 06/01